

What is claimed is:

Sub  
A1

1. A database management apparatus, comprising:  
an encryption key specification unit specifying  
5 whether a key for encryption of data of a column item  
of a database using a column key common among column  
items or a row key specific to each row;  
an encryption unit encrypting each column item  
of the database using a key specified by said  
10 encryption key specification unit; and  
a storage unit storing in memory the database  
encrypted by said encryption unit.
- 2 The apparatus according to claim 1, further  
15 comprising  
a database search unit encrypting data input for  
retrieval using a row key common among predetermined  
column items when column items encrypted using the  
common row key is to be retrieved, comparing the  
20 encrypted retrieving data with each item data of the  
encrypted database stored in the memory, and  
performing retrieving process.
3. The apparatus according to claim 1, wherein  
25 said encryption unit encrypts data of a

predetermined column item using a combination of a row key specific for each row and a column key common among corresponding column items.

5 4. The apparatus according to claim 1, wherein  
said encryption unit generates sequential vectors  
in a multidimensional space based on a predetermined  
function, and encrypting a database using the row key  
and the column key as a constant of the function in  
10 an encryption system using elements of the vectors as  
a key stream of encryption.

5. A database system which has a first information  
terminal containing a database, and a second  
15 information terminal requesting the first information  
terminal to search the database, and connects the  
first and second information terminals through a  
network, wherein:

20 on the first information terminal side, data of  
a first type of column item of the database is  
encrypted using a column key common among the column  
items, and data of a second type of column item is  
encrypted using a row key using a column key specific  
to each row;

25 when the second information terminal requests

009260-12102960

searching the database for the first type of column item, retrieving data input is encrypted using a column key common among the column items, and the encrypted retrieving data is transmitted to the first information terminal through the network; and

on the first information terminal side, the encrypted database is searched using the retrieving data, and the encrypted data obtained as a search result is returned to the second information terminal through the network.

6. The database management apparatus which manages a database in which data is encrypted using a column key common among predetermined column items, comprising:

an encryption unit encrypting input retrieving data using the column key when data is retrieved from predetermined column items; and

a retrieval unit retrieving data by comparing the encrypted retrieving data with each item data of the encrypted database.

7. The apparatus according to claim 1, comprising:  
a plaintext data obtaining unit obtaining plaintext data to be encrypted;

a vector generation unit sequentially generating vectors defined in a closed area of an  $n(n \geq 1)$ -dimensional space using a function determined using at least the column key or a row key; and

5 a logical operation unit performing a logical operation in bits units using the plaintext data obtained by said plaintext data obtaining unit and elements of the vectors generated by said vector generation unit, and generating encrypted data.

10 8. A computer-readable storage medium storing a program used to direct a computer to perform the process, comprising:

encrypting data of a first type of column item  
15 of a database using a column key common among the column items, and encrypting data of a second type of column item using a row key specific for each row; and  
searching encrypted database obtained as a result of the encrypting function.

20 9. A computer-readable storage medium storing a program used to direct a computer to perform the process, comprising:

encrypting input retrieving data using the column  
25 key when data is retrieved from predetermined column

005260-12402560

A1

items; and

retrieving data by comparing the encrypted  
retrieving data with each item data of the encrypted  
database.

5

10. A database management apparatus, comprising:

a first encryption unit encrypting data of a  
first type of column item of a database using a column  
key common among the column items, and encrypting data  
of a second type of column item using a row key  
specific for each row;

10

a second encryption unit encrypting the row key  
used in encrypting the data of the second type of  
column item of the database by said first encryption  
unit using another key common among rows; and

15

a storage unit storing in memory the database  
encrypted by said first encryption unit with the row  
key encrypted by said second encryption unit.

20

11. The apparatus according to claim 10, wherein

said row key is generated by a row number  
assigned to each row of said database and a random  
number.

25

12. An encryption apparatus according to claim 10,

009200" 42402900

A1

comprising:

a vector generation unit sequentially generating vectors defined in a closed area of an  $n(n \geq 1)$ -dimensional space using a function determined using each of the keys in the database management apparatus according to claim 10; and

a logical operation unit performing a logical operation in bits units using the plaintext data obtained by said plaintext data obtaining unit and components of the vectors generated by said vector generation unit, and generating encrypted data.

13. A database system having a first terminal unit for managing a database, and a second terminal unit for searching the database independent of the first terminal unit, wherein:

on the first terminal unit side, the database is encrypted and the encrypted database is stored in a portable storage medium, and the storage medium is distributed; and

on the second terminal unit side, the encrypted database is searched using the distributed storage medium, and data obtained as a search result is decrypted and displayed.

14. The system according to claim 12, wherein:

said first terminal unit encrypts data of a first type of column item of the database using a column key common among the column items, encrypts data of a second type of column item using a row key using a column key specific to each row, and encrypts the row key using another key common among rows; and

said encrypted database is stored with the row key after the encryption in a storage medium.

15. The system according to claim 12, wherein

said storage medium stores the encrypted database in said first terminal unit, and a predetermined program for searching encrypted database.

16. A computer-readable storage medium storing a program used to direct a computer to perform the process, comprising:

encrypting data of a first type of column item of a database using a column key common among the column items, and encrypting data of a second type of column item using a row key specific for each row; and

encrypting a row key used in encrypting data of a second type of column item of the database by said first encrypting function using another key common

A1 among rows.

17. An encryption system, comprising:

5 a rotation matrix generation unit generating an  
n-dimensional rotation matrix  $R_n (\Omega_n)$  for rotating a  
vector defined in a closed area of an  $n(n \geq 1)$ -  
dimensional space using each component of the vector  
and an angle  $\Omega_n$  depending on a parameter set  $P$  such  
that an  $(n-1)$ -dimensional rotation matrix  $R_{n-1} (\Omega_{n-1})$   
10 can be contained as an  $(n-1)$ -dimensional small matrix;

a vector generation unit generating a vector  $r_j$   
such that vectors  $r_j$  ( $j \geq 0$ ) sequentially generated  
using a nonlinear function containing at least the  
rotation matrix  $R_n (\Omega_n)$  cannot match each other in the  
15 n-dimensional space; and

a binary operation unit generating encrypted data  
by performing a binary operation using plaintext data  
and components of the vector  $r_j$  generated by said  
vector generation unit.

20

18. The system according to claim 16, wherein

said nonlinear function of said vector generation  
unit is a function containing a fixed vector for  
spatial translation of a rotation vector, and said  
25 vector generation unit sequentially generating vectors

009260"42402960



such that the generated vectors cannot match each other.

19. The system according to claim 16, wherein

5        said  $n$ -dimensional rotation matrix  $R_n (\Omega_n)$  used  
by said vector generation unit is generated by a  
product of an  $n$ -dimensional rotation matrices  
generated by changing insertion places of  $(n-1)$ -  
dimensional small matrix corresponding to an  $(n-1)$ -  
10       dimensional rotation matrix  $R_{n-1} (\Omega_{n-1})$ .

20. The system according to claim 16, wherein

      said binary operation (op) indicates that an  
exclusive logical sum operation (XOR) is performed  
15       after performing a scrambling operation  $S$ , represented  
by

$$op = XOR \cdot S$$

20       21. The system according to claim 16, wherein

      encrypted data  $C_j$  is generated by performing the  
binary operation on plaintext data  $M_j$  and a vector  
obtained by performing the binary operation on a  $j$ -th  
vector  $r_j$  generated by a nonlinear function used by  
25       said vector generation unit and a check sum  $\Sigma_{j-1}$  of  $(j-$

009260-12102960

1)-th generated encrypted data  $C_{j-1}$ .

22. A decryption system, comprising:

5 a vector generation unit generating vectors  $r_j$  such that vectors  $r_j$  sequentially generated using a nonlinear function containing at least an  $n$ -dimensional rotation matrix  $R_n (\Omega_n)$  for rotating a vector defined in a closed area of an  $n(n \geq 1)$ -dimensional space using each component of the vector and an angle  $\Omega_n$  depending on a parameter set  $P$  cannot  
10 match each other in the  $n$ -dimensional space;

an inverse binary operation unit receiving encrypted data, from an encrypting side, generated by performing a binary operation on plaintext data and  
15 components of a vector  $r_j$  generated by a method similar to a method of said vector generation unit, and decrypting the plaintext data by performing an inverse binary operation corresponding to an inverse operation to the binary operation using the vector  $r_j$   
20 generated by said vector generation unit and the encrypted data.

23. The system according to claim 21, wherein

25 said rotation matrix  $R_n (\Omega_n)$  is generated by said rotation matrix generation unit according to claim 17.

24. The system according to claim 21, wherein  
 said nonlinear function used by said vector  
 generation unit is a function containing a fixed  
 vector for spatial translation of a rotation vector,  
 5 and said vector generation unit sequentially generates  
 vectors such that the vectors cannot match each other.

25. The system according to claim 21, wherein  
 an n-dimensional rotation matrix  $R_n (\Omega_n)$  used by  
 10 said vector generation unit is generated by a product  
 of an n-dimensional rotation matrices generated by  
 changing insertion places of (n-1)-dimensional small  
 matrix corresponding to an (n-1)-dimensional rotation  
 matrix  $R_{n-1} (\Omega_{n-1})$ .

26. The system according to claim 21, wherein  
 said binary operation (op) indicates that an  
 exclusive logical sum operation (XOR) is performed  
 after performing a scrambling operation S, represented  
 20 by

$$\text{op} = \text{XOR} \cdot S; \text{ and}$$

said inverse binary operation ( $\text{op}^{-1}$ ) indicates  
 25 that an inverse operation  $S^{-1}$  inverse to the

009260-12102960

scrambling operation S is performed after performing an exclusive logical sum (XOR), represented by

$$op^{-1} = S^{-1} \text{ XOR}$$

5

27. The system according to claim 6, wherein a check sum  $\Sigma_{j-1}$  of a (j-1)-th received encrypted data  $C_{j-1}$  is generated, the binary operation is performed using a result of the generation and a vector  $r_j$  generated by the nonlinear function used by said vector generation unit, then the inverse binary operation is performed using a vector generated by the binary operation and a j-th received encrypted data  $C_j$ , thereby decrypting plaintext data  $M_j$ .

15

28. A vector generation system for use in a database management apparatus and an encryption/decryption system, wherein

20

when an n-dimensional rotation matrix R for rotation of a vector defined in a closed area of an  $n(n \geq 1)$ -dimensional space using each component of the vector and an angle depending on a parameter set P is generated, a plurality of rotation matrices of a smaller number of dimension are arranged as diagonal blocks, and pseudo-rotation matrices Q generated as

25

009260-12102960

0 elements are used in remaining portions.

29. The system according to claim 28, wherein

5 when an n-dimensional rotation matrix R for rotation of a vector defined in a closed area of an n(n≥1)-dimensional space using each component of the vector and an angle depending on a parameter set P is generated, a plurality of rotation matrices of a smaller number of dimension are arranged as diagonal  
10 blocks, and a matrix P formed by performing a similar transform represented by  $P = S \cdot Q \cdot S^T$  by a replacing matrix S on a pseudo-rotation matrices Q generated as  
0 elements are used in remaining portions.